Capital Asset Plan and Justification
Security and Privacy Considerations

OCIO Workshop

July 18, 2001

Security Policies and Guidance

- Computer Security Act of 1987
- Paperwork Reduction Act of 1995
- Clinger-Cohen Act
- NIST Special Publication 800-12, *"Introduction to Computer Security"*
- NIST Special Publication 800-14, *"Generally Accepted Principles and Practices for Security IT Systems"*
- OMB Circular A-130
- OCIO Guide to Capital Planning and Investment Control for Security (OCIO Web Site)
- **OCIO Interim Guidance**
- **OMB M-00-07, *"Incorporating and Funding Security in Information Systems Investments"***
- **Government Information Security Reform Act (GISRA) of 2000**

USDA Guidance for Security Plans (CS-002)

Requirements:

1. Address agency security management and structure
2. Identify agency security policies
3. Identify and discuss long-term security strategy
4. Address personnel security
    - Training and awareness
    - Rules of behavior
    - Clearances
    - Access control
5. Risk assessment
6. Contingency and disaster
7. Physical security

How to meet requirements:

- Develop and submit agency and system security plans

OMB Guidance

1. **Demonstrate Understanding of Life Cycle Security**
   - Design Phase Security Costs.
   - Production Phase Security Costs.
   - Ongoing/Maintenance Security Costs.
   - Additional costs for security more stringent than NIST requirements.

How to meet requirement:

- Security representative participates in Integrated Product Team for Investment.
- Conduct Security Analysis during design phase, then periodically thereafter.

OMB Guidance

2. **Demonstrate Understanding of System Risks**
   - Understand use and method for evaluating risk
   - Ensure controls are commensurate with risk
   - Identify additional controls for systems that promote or permit public access

How to meet requirement:

- Plan, conduct System Risk Assessment (Design Phase).
- Identify system vulnerabilities.
- Identify risks.
- Prepare Risk Mitigation Plan
- Incorporate Mitigation into system design
- Conduct Post-implementation Review(s)
- Correct security weaknesses as they are uncovered.

OMB Guidance

3. Identify "added" security controls for

- *Public Access Systems,*
- *Systems with External Access,*
- *Inter-connected System for which agency does not have direct control.*

How to meet requirement:

- Examine system design and determine cost for:
  - Facility to be used
  - Network connections
  - Processing centers
  - Access (Public, Remote, Partners)
  - Internet Requirements

OMB Guidance

4. Privacy and Confidentiality Must be Considered

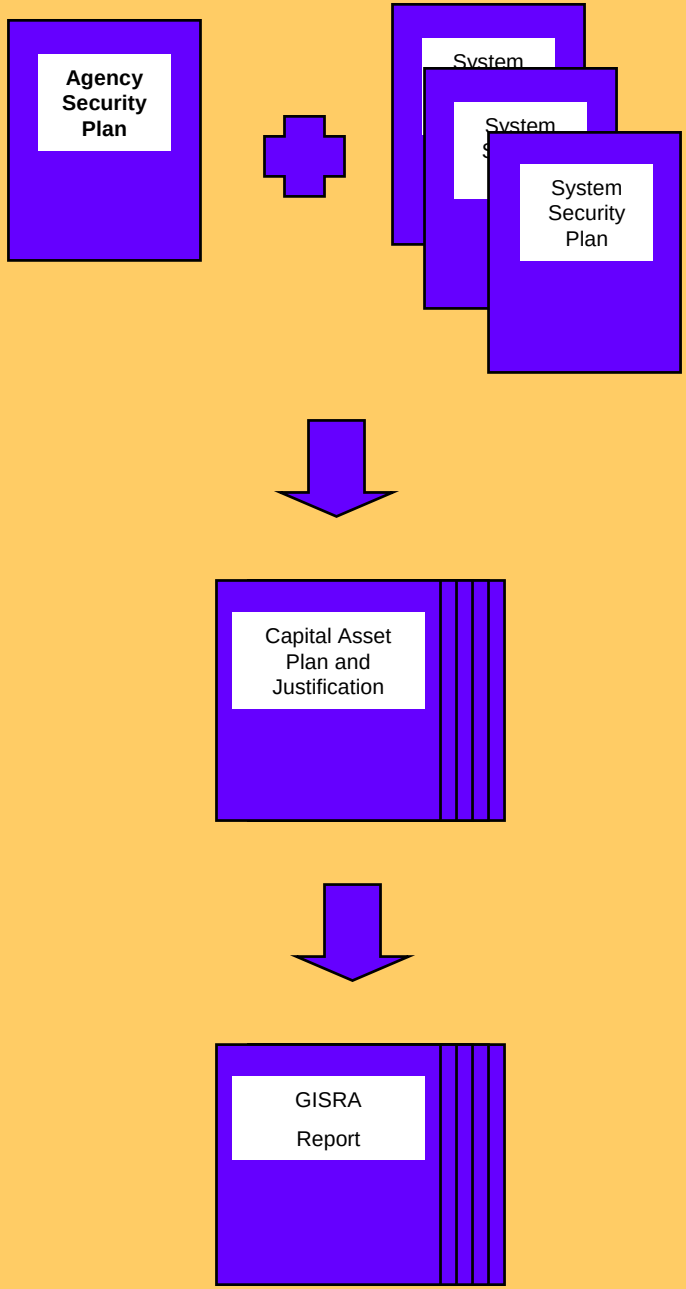
- Information on individuals must be necessary to mission
- Privacy Act Records must be protected
- Disclose on “need to know” basis and maintain records of disclosure
- Post Privacy Policy on Web
- Do not collect “Persistent Cookies”
- Handle shared data responsibly

How to meet requirement:

- Become familiar with USDA and OMB privacy guidance
- Examine data to ensure only mission essential personal data is being maintained
- Post Privacy Policy/Do not collect Persistent Cookies
- Secure and protect records, limit access
- Plan for costs of privacy requirements

GISRA Requirements

1. Agencies must incorporate security into system life-cycle
2. Annual Department-wide Security Plan
3. Annual Security/System Program Reviews
4. Annual Inspector General Report to OMB
5. Annual OMB report to Congress


Agency Security Plan
System
System
System Security Plan
Capital Asset Plan and Justification
GISRA
Report

"The Cyber Security Program Office will be conducting additional training on the security aspects of Capital Planning and Investment Control in the near future."